

09/579,035

RECEIVED
CENTRAL FAX CENTER

FEB 14 2007

Present Claims

1-373 (Canceled)

374. (Currently Amended) An Internet-based method of securing a computer communications network supporting a network computing device, said Internet-based method comprising the steps of:

- (a) downloading encrypted content over a global network to a memory storage device within said network computing device;
- (b) embodying a global synchronization chip into said network computing device,
- (c) programming the global synchronization chip in said network computing device with a set of predetermined time and space (TS) coordinates so as to enable said network computing device to decrypt said encrypted content only when said network computing device is temporally and spatially present at said TS coordinates; and
- (d) disposing said network computing device at said predetermined TS coordinates so as to automatically enable said network computing device to decrypt said encrypted content at a time different from said downloading and wherein said content is visually or sonically presented by the device; and

(e) providing a web-based device trajectory monitoring server to allow monitoring of TS trajectories of each network computing device, and to determine when and where received encrypted radio messages have been decrypted and visually or sonically displayed by the network computing device.

375. (Previously Presented) The Internet-based method of claim 374, wherein step (d) comprises said network computing device transmitting a digitally-signed data package to a TS-stamping tracking server for receiving said digitally-signed data package and processing the same collect data indicative that said network computing device is present at said predetermined TS coordinates and automatically transmitting a digitally-signed package back to said enabled network computing device to access said communications network or subnetwork thereof (or WWW server connected thereto).

09/579,035

376. (Currently Amended) An Internet-based method of securing a computer communications network supporting a network computing device, said Internet-based method comprising the steps of:

- (a) downloading encrypted content over a global network to a memory storage device within said network computing device;
- (b) embodying a global synchronization chip into said network computing device so as to provide a GSU-enabled network computing device, and
- (c) programming the global synchronization chip in said network computing device with a set of predetermined time and space (TS) coordinates so as to decrypt said encrypted content and fully enable said network computing device to access said communications network or subnetwork thereof (or WWW server connected thereto) when said network computing device is temporally and spatially present at said TS coordinates, and partially enable said network computing device to partially access said communications network, ~~or a subnetwork said communications network, or a thereof (or WWW server connected to said communications network, thereto)~~ when said network computing device is not temporally and spatially present at said TS coordinates;
- (d) disposing said network computing device outside of said predetermined TS coordinates so as to partially enable said network computing device to partially access said communications network or subnetwork thereof;
- (e) disposing said network computing device at said predetermined TS coordinates so as to automatically enable said network computing device to decrypt said encrypted content at a time different from said downloading and wherein said content is visually or sonically presented by the device;
- (f) tracking the exact location of said network computing device with a TS-stamping tracking server, and
- (g) notifying authorities so that said authorities have information needed to apprehend the person using the same without authorization; and

09/579,035

(h) providing a web-based device trajectory monitoring server to allow monitoring of TS trajectories of each network computing device, and to determine when and where received encrypted radio messages have been decrypted and visually or sonically displayed by the network computing device.

377. (Currently Amended) An Internet-based method of securing a computer communications network having a plurality of network computing devices, said method comprising the steps of:

- (a) downloading encrypted content over a global network to a memory storage device within at least one of said network computing devices;
- (b) embodying a global synchronization device into each network computing device so that its access to decrypt said encrypted content and access to a particular communications/computer network, subnetwork or WWW site can be securely enabled by a TS-stamping tracking server only upon the generation of a unique time-space stamp by the GSU-chip corresponding to a predetermined location over which the network computing device is enabled;
- (c) disposing said network computing device at said predetermined TS coordinates so as to automatically enable said network computing device to decrypt said encrypted content at a time different from said downloading and wherein said content is visually or sonically presented by the device; and
- (d) disposing said network computing device at said predetermined location so that said network computing device is enabled by said TS-Stamping Based Tracking Server to access a prespecified communication subnetwork or WWW server; and

(e) providing a web-based device trajectory monitoring server to allow monitoring of TS trajectories of each network computing device, and to determine when and where received encrypted radio messages have been decrypted and visually or sonically displayed by the network computing device.

09/579,035

378. (Currently Amended) An Internet-based method of securing a computers communications network by embodying a global synchronization chip in a network computing device which is used to access a particular communications network, subnetwork, ~~(sub)network~~ or WWW site, the method comprising,

downloading encrypted content over a global network to a memory device within said network computing device; and

partially enabling said network computing by a TS-stamping tracking server when the network computing device is present outside of a predetermined location, or a predetermined time interval,

tracking, with the TS-stamping tracking server, the exact location of said network computing device;

automatically enabling said network computing device to decrypt said encrypted content at a time different from said downloading and visually or sonically presenting said content when said network computing device is present within a predetermined location and a predetermined time interval, and notifying authorities to apprehend the person using said network computing device without authorization; and

providing a web-based device trajectory monitoring server to allow monitoring of TS trajectories of each network computing device, and to determine when and where received encrypted radio messages have been decrypted and visually or sonically displayed by the network computing device.

379. (Currently Amended) An Internet-based system for securing a computer communications network supporting a network computing device, said Internet-based system comprising:
a globally synchronized network computing device, said globally synchronized network computing device including

a global synchronization chip capable of generating time and space (TS) coordinates indicative of the time and space coordinates of said global synchronization chip in relation to a globally referenced

09/379,033

coordinate system, and

a network interface for providing an interface between said globally synchronized network computing device and a computer communications network or subnetwork thereof;

wherein said global synchronization chip is programmed with a set of predetermined time and space (TS) coordinates so as to enable said globally synchronized network computing device

to access prestored encrypted content that was downloaded over a global network within a memory device of said network computing device; and

to access said computer communications network or subnetwork thereof only when said globally synchronized network computing device is temporally and spatially present at said TS coordinates; and

a web-based device trajectory monitoring server to allow monitoring of TS trajectories of each network computing device, and to determine when and where received encrypted radio messages have been decrypted and visually or sonically displayed by the network computing device.